

## <<缓冲区溢出攻击>>

### 图书基本信息

书名：<<缓冲区溢出攻击>>

13位ISBN编号：9787302139423

10位ISBN编号：7302139423

出版时间：2006-12

出版时间：清华大学出版社

作者：福斯特

页数：409

字数：606000

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<缓冲区溢出攻击>>

### 内容概要

对一些恶名昭彰的Internet攻击（如SQL Slammer和Blaster蠕虫）的取证调查，显示了缓冲区溢区是高明的黑客进行攻击时选择的弱点。

这些蠕虫会使Internet速度减慢甚至瘫痪，并且需要花费数十亿美元清除它们。

目前，威力更强的、更阴险的威胁已经以“Custom exploits”的形式出现，即每一次攻击的exploit都是不同的，从而使exploit更难以发现和防范。

这样既不容易记住其名称，也没有相关的媒体报道，但却会带来严重的灾难。

本书清楚地说明，防范无穷无尽的缓冲区溢出攻击变种的唯一方法是对所有的应用程序进行完善的设计、编码和测试。

这本书是目前用于检测、剖析和防止缓冲区溢出攻击的唯一的书籍。

## <<缓冲区溢出攻击>>

### 作者简介

James C.Foster是CSC的全球安全解决方案开发部门的副主任，在加入CSC前，Foster是Foundstone公司的开发和研究部门的负责人，他全面负责公司的产品、咨询以及研发方面的指导。在加入Foundstone前，Foster是Guardent公司的高级顾问和资深研究员，同时兼任Information Security杂志的编辑。

## &lt;&lt;缓冲区溢出攻击&gt;&gt;

## 书籍目录

第 部分 扩展缓冲区溢出 第1章 缓冲区溢出的基本概念 1.1 简介 1.2 软件安全危机 1.3 缓冲区溢出的增加 1.4 exploits与缓冲区溢出 1.5 定义 1.6 小结 1.7 快速解决方案 1.8 网站链接 1.9 邮件清单 1.10 常见问题 第2章 理解shellcode 2.1 简介 2.2 shellcode概述 2.3 空字节问题 2.4 实现系统调用 2.5 远程shellcode 2.6 本地shellcode 2.7 小结 2.8 快速解决方案 2.9 网站链接 2.10 邮件清单 2.11 常见问题 第3章 编写shellcode 3.1 简介 3.2 shellcode示例 3.3 重用程序变量 3.4 操作系统间的shellcode 3.5 理解已有的shellcode 3.6 小结 3.7 快速解决方案 3.8 网站链接 3.9 邮件清单 3.10 常见问题 第4章 Win32汇编语言 4.1 简介 4.2 应用程序的内存布置 4.3 Windows汇编 4.4 小结 4.5 快速解决方法 4.6 网站链接 4.7 常见问题 案例分析1.1 FreeBSD NN Exploit代码 案例分析1.2 xlockmore用户提供的格式化字符串 案例分析1.3 使用Winsock的Frontpage的拒绝服务 案例分析1.4 FreeBSD上的cURL缓冲区溢出 第 部分 缓冲区溢出解析 第5章 堆栈溢出 5.1 简介 5.2 Intel x86结构和机器语言基础 5.3 堆栈溢出和它们的利用 5.4 什么是Off-by-One 溢出? 5.5 寻找堆栈溢出的挑战 5.6 小结 5.7 快速解决方案 5.8 网站链接 5.9 邮件清单 5.10 常见问题 第6章 堆腐烂 6.1 简介 6.2 简单堆腐烂 6.3 高级堆腐烂—Doug Lea malloc 6.4 高级堆腐烂——System V malloc 6.5 应用程序防御 6.6 小结 6.7 快速解决方案 6.8 网站链接 6.9 常见问题 第7章 可移植的网络编程 7.1 简介 7.2 什么是格式化字符串 7.3 使用格式化字符串 7.4 误用格式化字符串 7.5 利用格式化字符串缺陷的挑战 7.6 应用程序防御 7.7 小结 7.8 快速解决方案 7.9 网站链接 7.10 常见问题 第8章 Windows缓冲区溢出 8.1 简介 8.2 小结 8.3 问题快速解决方案 8.4 网站链接 8.5 常见问题 案例分析2.1 Linux中的cURL缓冲区溢出 案例分析2.2 异常客户端密钥远程缓冲区溢出漏洞 案例分析2.3 X11R6 4.2 XLOCALEDIR溢出 案例分析2.4 微软MDAC拒绝服务漏洞 案例分析2.5 本地UUX缓冲区在HPUX上溢出 第 部分 查找缓冲区溢出 第9章 从源代码中找出缓冲区溢出 9.1 简介 9.2 源代码分析 9.3 免费开放源代码工具 9.4 Application Defense——企业开发版 9.5 Secure Software公司 9.6 Ounce Labs公司 9.7 Fortify Software公司 9.8 小结 9.9 快速解决方案 9.10 网站链接 9.11 常见问题 案例分析3.1 InlineEgg I 案例分析3.2 InlineEgg II 案例分析3.3 Seti@Home Exploit 代码 案例分析3.4 微软公司CodeBlue Exploit代码 附录A 完整的数据换算表 附录B 有用的系统调用函数

## <<缓冲区溢出攻击>>

### 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>